VZCZCXYZ0000
PP RUEHWEB

DE RUEHBS #1140/01 2291206
ZNR UUUUU ZZH
P 171206Z AUG 09
FM USEU BRUSSELS
TO RUEHC/SECSTATE WASHDC PRIORITY
RUCPDOC/USDOC WASHDC PRIORITY
RHMFIUU/DEPT OF HOMELAND SECURITY WASHINGTON DC PRIORITY
RUEAWJA/DEPT OF JUSTICE WASHDC PRIORITY
INFO RHEHNSC/NSC WASHDC
RHMFIUU/HOMELAND SECURITY CENTER WASHINGTON DC
RUEKJCS/DOD WASHDC
RUEAFCC/FCC WASHDC
RUCNMEU/EU INTEREST COLLECTIVE
RUEAORC/US CUSTOMS AND BORDER PROTECTION WASHINGTON DC
RUEADRO/HQ ICE DRO WASHINGTON DC
RUEATRS/DEPT OF TREASURY WASHDC
RHMFIUU/FBI WASHINGTON DC
RUEABND/DEA HQS WASHINGTON DC
RUEAIIA/CIA WASHINGTON DC
RUEHSS/OECD POSTS COLLECTIVE

UNCLAS USEU BRUSSELS 001140

SENSITIVE
SIPDIS

STATE FOR EEB/CIP, EUR/ERA, L, INL, S/CT
DEPT PLEASE PASS FTC AND FDA
USDOC FOR ITA ROBIN GAINES-DEATS, TA DOUG DEVEREAUX, NTIA CHRISTINA SPECK
DOD FOR OSD SUPPLY CHAIN INTEGRATION KATHLEEN SMITH
FCC FOR TRACEY WEISLER
TREASURY FOR TFTP

E.O. 12958: N/A
TAGS: ECON ECPS EINT BEXP KJUS KTFN TINT PREL ETTC EUN
SUBJECT: THE MANY SIDES OF DATA PRIVACY: MANAGING RISING TENSIONS WITH THE EU

REF: BRUSSELS 1073

¶1. (SBU) SUMMARY: European privacy and data protection concerns continue to jeopardize our commercial, law enforcement, intelligence and foreign policy objectives. Data privacy is an area of growing complexity and touches ever more U.S. interests, from the visa waiver program to e-commerce. We should enhance and coordinate U.S. outreach in the coming year to address the variance between U.S. and EU approaches to privacy protections. The USG should develop an interagency approach to the EU on both commercial and law enforcement data protection/privacy issues. Such an approach should aim to ensure that data privacy rules will not hinder economic growth, endanger global economic recovery, or discourage greater law enforcement cooperation. For now, we are already encountering problems in these areas. END SUMMARY.

Overview

¶2. (SBU) The financial crisis has provided a potent reminder that the global economy is increasingly interconnected and dependent on information technology. Personal data exchange is an ever-larger part of the digital economy. Trade and investment depending on the transfer of personal data across the Atlantic reaches hundreds of billions of dollars annually. Privacy is also a political issue, connected in European minds with respect for fundamental democratic values.

¶3. (SBU) The European Union has a strict regulatory regime in place for the protection of personal data ("data protection") in the economic and social sphere. Under current EU treaty structures, this economic and social sphere falls within what is referred to commonly as the "First Pillar," that is, EU powers that derive from the original 1957 Rome Treaties and deal with economic and trade issues, rather than the "Second Pillar (Common Foreign and Security Policy) or "Third Pillar" (Justice and Home Affairs) that have evolved over the last 15 years.

¶4. (SBU) The EU- and Member State-level institutions that play a role in the data protection space have also been generating data protection challenges and concerns in the "Third Pillar" context that includes law enforcement. There are also proliferating data protection issues related to the "Second Pillar" of Common Foreign and Security Policy (CFSP), notably regarding implementation of targeted economic sanctions. (Note: these EU treaty distinctions

would change after final ratification of the proposed "Lisbon Treaty," which could occur by the end of 2009. End note.)

¶5. (SBU) Damage to U.S. political and commercial interests over EU data protection and privacy issues has raised concerns in our law enforcement community for some years. EU data protection assumptions and dictates delayed more formal U.S.-EU judicial and law enforcement cooperation over the past decade. For example, they delayed U.S. entry into and full implementation of cooperation agreements with Europol (EU police coordination unit) and Eurojust (EU judicial coordination unit). The pending transfer out of the United States of Society for Worldwide Interbank Financial Telecommunication (SWIFT) financial transaction records is another example. This action will make more difficult our ability to obtain information to track terrorist financing. Also, U.S.-legislated 100 percent scanning of cargo shipments has already run into data protection obstacles in a European test-run of container scanning. Some fear that differences between European and U.S. data protection regimes will perpetuate dangerous misperceptions of U.S. values in Europe and beyond. Residual uncertainty about the "adequacy" of the U.S. privacy regime might have a "chilling effect" in some quarters on the exchange of vital law enforcement information.

EU Legislation: First Pillar

¶6. (SBU) The EU's 1995 Directive on the Protection of Personal Data (DPD) sets out principles for the protection of data that apply across the whole of the EU's First Pillar. It requires that each Member State set up an independent data protection authority (DPA) charged with enforcement of these principles. Critically, the DPD also bans the transfer of personal data to third countries that are not deemed to have an "adequate" system for protecting personal data. The United States does not enjoy a blanket "adequacy" finding, largely because the United States does not have a single independent DPA. Consequently, the vast amount of transatlantic economic activity that implies the transfer of personal data from the EU to the United States relies on a limited set of exceptions set out in the DPD, as well as on sector-specific agreements: the Safe Harbor agreement, the Passenger Name Record (PNR) agreement, and Terrorist Finance Tracking Program/SWIFT. (Note: The SWIFT pending tr of U.S. territory derives`ta protection concernsQ@(.

¶7. (U) The 2002 Dg of Personal Data andrivacy in the Electronic C the "ePrivacy Directive"nf electronic communicatelecommunications andders to destroy traffic longer required for@h`rQ`l Q rs with a pool of avaitigation of suspects,
¶9. (U) The May 2009 Qio Frequency Identification Device RFID) Privacy Recommendation clarifies the a0plicability of the DPD and the ePrivacy Direcive to RFID systems. It also recommends the uQe of Privacy Impact Assessments (PIQs) by retailers in determining whether RFID applications that retailers use could pose Q threat to consumer privacy. In such cases, an opt-in is recommended - i.e., retailers ar encouraged to deactivate RFID tags a the point of sale.

EU Legislation: Third Pillar

¶10. (U) The EU Council's November 2008 Framework Decision on the Protection of Personal Data Processed in the Context of Police and Judicial Co-operation in Criminal Matters (the "Framework Decision") is the most recent EU development of data protection policy in the Third Pillar. The Framework Decision must be fully implemented by November 27th, 2010. Broadly speaking, the decision parallels the DPD, while adapting it to the specific nature of the Third Pillar. (Note: A mistaken belief in Europe is that the U.S. law enforcement data privacy system does not provide judicial access for non-U.S. persons to view their data or challenge its correctness. This widely circulating "urban myth" is being used to generate skepticism in Europe about U.S. efforts to collaborate with the EU on exchanges of law enforcement information, for example. End note).

EU Legislation: Next Steps

¶11. (U) At a May 19-20 data protection conference, the European Commission announced it will run a public consultation from July until the end of 2009 on the EU legislative framework for privacy. The conference and consultation are widely seen as the first steps in a process that may culminate in a proposed revision of the DPD. The UK DPA recently published a study that called for wide-ranging changes to the EU legislation. Commission officials have said that they hope to unify the First and Third Pillar legislative frameworks after the ratification of the Lisbon Treaty. Such an approach is supported by many privacy advocates. (COMMENT: Full unification of

the First and Third Pillar frameworks may have implications for U.S. commercial and law enforcement interests. For example, a European individual's purchase over the Internet of materials used to construct a terrorist bomb could be a key element in a U.S. prosecution, but the information might be made more difficult for U.S. law enforcement to detect and access because of European data privacy protections. (END COMMENT)

EU Institutional Players

¶12. (U) Privacy-related responsibilities are spread across a range of European Union institutions. The Commission lead on data protection is the Directorate General for Justice, Freedom and Security (JLS). (NOTE: JLS took this over from DG Internal Market (MARKT) earlier this decade. END NOTE.) However, DG Information Society and Media (INFSO) leads for the Commission on RFID issues and on the ePrivacy Directive. DG Public Health and Consumer Protection (SANCO) leads on policy development related to consumer protection, such as behavioral advertising. Both DG SANCO and DG MARKT play a role in policy development in eCommerce.

¶13. (U) The office of the European Data Protection Supervisor (EDPS), established in 2001, is independent of the Commission and is responsible for making "sure that the fundamental right to protection of personal data is respected by the EU institutions and bodies." (See http://ec.europa.eu/justice_home/fsj/privacy/eusupervisor/index_en.htm. The EDPS, currently Peter Hustinx, also has a role in advising EU institutions on data protection policy and cooperating with the Member States' DPAs. Mr. Hustinx's profile and role have grown considerably over the EDPS' eight-year existence. He has sought to expand the scope of his activities from the First to the Second and the Third Pillars.

¶14. (U) In addition, Member State DPAs meet together in a committee set up by Article 29 of the DPD. This "Article 29 Working Party" (A29WP, or WP) seeks common interpretations of EU data protection law and shares information and best practice in its First Pillar area of responsibility. It adopts non-binding but influential opinions.

¶15. (U) Under current EU treaty structures, the European Parliament (EP) has co-decision legislative powers on First Pillar data protection, following a Commission proposal. This refers to the process whereby a Commission proposal for an EU directive or regulation (the two principal forms of EU legislation) is sent forth for approval by the 27 Member States; after Member State approval, the proposed directive or regulation can be modified by the EP. Absent a Commission-proposed directive or regulation, the EP's formal powers are limited. But politically, the media-savvy EP has cultivated a high profile role on data protection policy through public hearings, resolutions, non-binding statements, opinions, and lobbying the Council and Commission for action in both the First and Third Pillar arenas.

Policy Development Efforts

¶16. (U) The European Commission is conducting a long-term review of the legislative framework for data protection, and is working in several areas related to privacy. The Commission is interested in the concept of the "Internet of Things" (also known as the "networked environment"). The Commission believes that future proliferation of electronically networked objects will transform society and the economy, with major governance implications, including in the area of privacy.

¶17. (U) The Commission continues its Safer Internet work, aimed in particular at protecting children from harmful content and relationships on the Internet. It has also begun work on the consumer protection aspects of privacy in social networking, criticizing the broad use of personal data currently made by Internet social networking and related services.

¶18. (U) The Commission is also looking at structural aspects of personal data storage on the Internet. Cloud computing, in which the geographical location of increasing amounts of consumer data is dynamic or changing, raises questions of jurisdiction. Another structural issue is the use made by service providers of data collected on individuals in order to provide personalized, or behavioral, advertising.

¶19. (U) The USG continues active engagement in the development of the APEC Privacy Framework, which some see as a more flexible alternative to wholesale adoption of the EU approach. The OECD and the Council of Europe (CoE) have strong records of privacy policy

development and are likely to continue work in the area. In July 2008, the CoE announced the opening of its binding international instrument, Convention 108, to non-member countries. However, USG internal organization is a hurdle to full U.S. participation.

Political Tensions Linger and Grow

¶20. (SBU) It is generally understood in Brussels (with a few exceptions) that U.S. privacy legislation long predates that of the EU. The FTC is well respected in Europe as an effective and experienced privacy regulator. European policymakers overwhelmingly agree that cooperation with the United States on data protection is essential. Much more importance is attached to the transatlantic relationship in this regard than to EU relations with other countries or regions. Adequacy findings do exist for the Safe Harbor, and specific agreements have been reached for the U.S.-EU Passenger Name Record (PNR) and SWIFT. These agreements have survived heated debates in the public and private sectors. (NOTE: Nevertheless, as mentioned previously, SWIFT is now moving its U.S.-located data banks out of the United States to Europe due to personal data protection concerns. END NOTE). Dialogue with the EU is relatively strong in both the First and Third Pillar areas (through the annual Safe Harbor conferences and the High Level Contact Group "HLCG", respectively).

¶21. (SBU) Many privacy concerns have been surmounted through U.S. Treasury's representations to the EU on the Terrorist Finance Tracking Program (TFTP), which previously caused a major public controversy involving Belgian company SWIFT. After receiving the study report of the Commission-designated independent examiner, EU Justice, Freedom and Security (JLS) Commissioner and Vice-President Jacques Barrot was effusive in his public praise of the TFTP's scrupulous attention to data privacy.

¶22. (SBU) Nevertheless, there remains a lingering perception in EU circles that the United States does not protect personal data as well as the EU. This is manifested, for example, in public criticism of the lack of cross-sectoral U.S. privacy legislation, including the privacy rules and practices of the U.S. Government, and a lingering misperception that the FTC as an agency and the Privacy Officers of our various Departments lack political independence.

HLCG on Third Pillar Data Privacy

¶23. (SBU) Following the above recent controversies and others, the United States and EU agreed to establish an experts' forum in 2007 to address Third Pillar (law enforcement rather than commercial) data privacy concerns. This group, the "High Level Contact Group (HLCG)", with representatives from the U.S. Departments of State, Justice and Homeland Security and from the EU Presidency, Council Secretariat and Commission identified a set of 15 principles common to all effective data protection and privacy systems. The principles were developed to work across the very different EU and U.S. systems; the EU system of a single Framework Decision to be implemented by all 27 Member States, and the U.S. system that is a combination of different laws, regulations, mechanisms and branches of government.

¶24. (SBU) Under the HLCG, and as instructed by the U.S.-EU JHA Ministerial, U.S. and European officials agreed to work toward a binding international agreement codifying these principles. This binding international agreement would be intended both to provide the template of these identified data privacy principles for insertion into any relevant U.S.-EU agreements to be negotiated in the future and also to dispel any lingering uncertainties by effectively declaring our mutual recognition of the "adequacy" of the U.S. and EU data privacy regimes. The U.S. interagency is in accord on what needs to be done through the HLCG.

¶25. (SBU) However, the EU refuses to negotiate formally until uncertainty over the Lisbon Treaty is resolved. (NOTE: The issue here is that when the Lisbon /Treaty is ratified by all Member States and takes effect, the European Parliament will have some decision-making authority that it does not now enjoy, over many JHA issues. Accordingly, the Commission argues that it does not want to alienate the Parliament by taking rapid, conclusive action on sensitive issues that it would otherwise, a few months later, have to submit to the Parliament for approval. END NOTE). Further, and prior to any formal negotiation, the Commission argues that the U.S. Administration must amend the 1974 Privacy Act to grant Europeans formal redress rights equivalent to those of U.S. citizens. (NOTE: The Safe Harbor program, though generally considered a successful mechanism for allowing transfers of personal data to the United States under the DPD, is criticized for similar reasons of perceived

asymmetry between Americans' rights in Europe and Europeans' rights in the United States. END NOTE.)

¶26. (SBU) COMMENT: This insistence reflects a European public misperception of the U.S. privacy regime for law enforcement records. The misconception ignores the whole purpose of the HLCG - that while our system differs from Europe's in not relying on a single law, it is nonetheless very effective. U.S. officials have repeatedly provided verbal and written explanations of the means of judicial redress available to all persons in the U.S. system. Even the most vocal challengers concede that their concern with the distinction drawn in the 1974 Act is more symbolic than real. At the same time, EU counterparts have not responded to the U.S. request for an explanation of how the Third Pillar data protection Framework Decision is being implemented in the Member States and

what judicial redress is available. However, the Swedish EU Presidency has proposed an experts' seminar this Fall to examine what redress is available in both EU Member States and in the United States, to finally dispel this misconception and uncertainty. END COMMENT.

Economic and Other Impacts on U.S. Firms
----------27. (SBU) Ongoing tensions protection and privac@.S. interests that are sure. For example, pri costs are higher becausQ`ks an EU "adequacy" findin@ncreasing pressure to a the United States benmer base perceives tped there is not safe. USE`able anecdotal evidence of business and being ors in Europe because of` eQpb``Ql@elgian action, appealQ global implication3and for broader human rights concerns (if other countries make similar request for Yahoo! data based on the same argumeQt) (REFTEL). In broader terms, the potential cost to the public of impairment in the transalantic law enforcement exchange of terrorismand international organized crime informationcould be enormous and/or tragic.

Underlyin Issues That Affect EU Policy Directins
---------- -----

¶29. (SBU) Many vocal critics arQ dissatisfied with the Commission DG JLS policy lead on privacy, because JLS has no direct responsibility for consumer protection, nor for economic or technological aspects of data protection. JLS-developed policy reflects the internal tension between civil liberties and law enforcement. Furthermore, the multiplicity of DGs and Commissioners leading on different aspects of privacy policy causes confusion internally and in the stakeholder community.

¶30. (SBU) The Commission has failed to exercise a strong policy leadership role vis-a-vis other EU institutions. In this vacuum, the European Data Protection Supervisor and the Article 29 Working Party have asserted expansive roles. These bodies regularly make high-profile public statements on areas outside of their formal competence (including the HLCG and Third Pillar issues). Their interpretations of legislation tend to give primacy to civil liberties-based approaches for the EU's Single Market, consumers, or law enforcement, and have gone largely unchallenged by the Commission.

¶31. (U) EU implementation of the DPD has seen significant harmonization problems, such as the development of rules governing the adoption and approval of "Binding Corporate Rules" (BCRs) by multinational companies. Although nine Member States have agreed to recognize each other's BCR approvals, no company has ever received approval from all 27 Member States for its BCRs.

¶32. (U) Also, enforcement of EU data protection laws has been patchy, and processes lack transparency. DPAs' resource levels and legal powers vary from country to country. Many stakeholders, including Member State DPAs, recognize that too much effort has been spent on bureaucratic aspects of enforcement, such as checking contracts used for data transfers to third countries, rather than systematic market surveillance.

¶33. (SBU) Also, many stakeholders question the concept of Third Pillar "adequacy", because this currently includes only a small number of jurisdictions (Switzerland, Argentina, Canada, and the Channel Islands) and excludes many vital economic partners (such as the United States) that enjoy strong traditions of democracy, civil liberties, and the rule of law. Many regard the concept as a test of similarity rather than adequacy.

¶34. (SBU) U.S. and European industry figures argue that the EU legislative framework for data protection lacks coherence. For example, the ePrivacy Directive requires Internet firms to delete traffic data when it is no longer needed for billing purposes, in apparent contradiction to the DRD's requirement that they retain the

data for up to two years.

Comment and Recommendations

¶35. (SBU) The Lisbon Treaty would significantly change EU "Pillar" decision-making structures, increasing the EP's role and shifting power bases in ways not yet fully understood. Lisbon will not change, however, the fundamentally evangelical character of European institutions' promotion of EU integration. EU institutions are structured to facilitate the spread of EU norms beyond EU borders. Across the full range of EU activities (from product safety, climate change, and chemicals regulation to human rights and free and fair elections), the EU actively pushes its methods for adoption by third countries in a way designed to make the EU standard the global standard. Not surprisingly, such standards in different fields tend to favor EU economic and cultural norms, rather than U.S. or other norms that may differ from those in Europe. Data protection, where the EU promotes its data protection/privacy system internationally as the "gold standard", is no exception. European DPAs are leading work among international privacy regulators to adopt international data protection standards.

¶36. (SBU) This structural dynamic presents a significant challenge to the United States, but the coming year also offers a critical opportunity. Political leadership has changed in the United States and is changing in the EU (including this year a new Parliament and Commission in Brussels), progress is being made on EU-led international data protection standards, and discussions on the legislative framework for privacy continue on both sides of the Atlantic.

¶37. (SBU) The USG should take advantage of these developments to define, organize, and implement a comprehensive interagency strategy to engage the EU on both commercial and law enforcement privacy and data protection issues as soon as possible. Such a strategy would have two primary objectives: first, to correct mistaken perceptions of U.S. privacy protection in both the public and private sectors; and second, to secure major improvements in the reciprocal understanding of both the U.S. and EU approaches to privacy and data protection through political, regulatory, and experts' dialogues. Such an approach could help minimize risks that new rules in this area will hinder economic growth, endanger global economic recovery, and discourage greater bilateral law enforcement cooperation. These objectives would be best achieved with the committed support of an

interagency group of senior Administration officials.

Key Opportunities for Engagement

¶38. (U) USEU recommends that a coordinated U.S. interagency approach might best be served by focusing on upcoming opportunities for potential U.S. stakeholder participation in EU policy discussions and processes. These include:

-- Final Adoption of the EU telecoms package including data breach amendments to the ePrivacy Directive (Brussels/Strasbourg): date TBD

-- Swedish Presidency expert seminar on effective redress available in the United States and in EU Member States (Brussels): date TBD

-- Meeting of the High-Level Contact Group (HLCG) (Brussels): date TBD

-- JHA Ministerial (Washington, DC): October 27-28

-- International Conference of Data Protection Authorities (Madrid): November 4-7

-- European Federation of Consumer Organizations conference on data protection (Brussels): November 12

-- Annual U.S.-EU Safe Harbor Conference (Washington): November 16-18

-- European Commission consultation on the legislative framework for data protection and possible associated events (Brussels): December 31

MURRAY